

REMARKS

Applicants respectfully request reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. Claims 29, 31, 36, 38, 42, and 44 have been amended. Claims 33, 34, 40, and 46 have been canceled. Claims 1-28 and 48-89 were previously canceled. Applicants respectfully submit that no new matter has been added. The elements of now canceled Claims 33, 34, 40, and 46 have been incorporated into Claims 29, 36, and 42. Claims 31, 38, and 44 have been amended based on the amendment to Claims 29, 36, and 42. Claims 29-32, 35-39, 41-45, and 47 are now pending in this application.

Rejection of Claims 29-47 Under 35 U.S.C. § 103

On page 3 of the Office Action, Claims 29-47 were rejected under 35 U.S.C. § 103 as being unpatentable over an article titled *Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses* by Montenegro *et al.* (Montenegro) in view of U.S. Patent No. 6,067,621 to Yu *et al.* (Yu). As stated previously, the elements of now canceled Claims 33, 34, 40, and 46 have been incorporated into Claims 29, 36, and 42. Applicants respectfully disagree that Montenegro and Yu, alone and in combination, teach or suggest all of the claim elements as recited in at least independent Claims 29, 36, and 42, as amended.

Independent Claim 29 recites in part:

- (a) identifying a number of identifications allowed;
- (b) identifying a secret value at a first device, wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed;
- ...
- (j) comparing the identified number of confirmations performed with the identified number of identifications allowed; and
- (k) based on an outcome of the comparison, identifying a second secret value at the first device and repeating (c)-(i) replacing the identified secret value with the identified second secret value.

Independent Claims 36 and 42 recite a similar feature.

On pages 4-5 of the Office Action, the Examiner apparently acknowledges that Montenegro does not teach, suggest, or describe at least the claim elements recited above. Relative to Yu, on page 4 of the Office Action, the Examiner states (with emphasis added through underlining and bolding):

Yu discloses ..., wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the **secret value** is changed (see, Fig. 6, Numerals 640 and 660 and also see, Column 10, lines 43-61, system uses a new **random number** when N reaches zero) and further discloses at the server side identifying a number of confirmations previously performed between the first device and the second device (see Fig. 7, and also see, Column 10, lines 63-67).

On page 5 of the Office Action, the Examiner states (with emphasis added through underlining and bolding):

the combination of Montenegro and Yu further discloses comparing the identified number of confirmations performed with the identified number of identification allowed; and based on outcome of the comparison, identifying a **second secret value** at the first device (see, Yu, Column 10, lines 43-61, system uses **a new random number** when N reaches zero).

Applicants respectfully submit that Yu does not teach “wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed” or “based on an outcome of the comparison, identifying a second secret value” as recited in Claims 29, 36, and 42.

At the cited sections, Yu states:

The counter value N is reduced by one each time a password is generated at step 650. The terminal 120 then determines whether the reduced value is 0 at step 640. When the value becomes 0, the process returns to an initial stage. The random number is usually increased by one and initialized when N becomes 0. In the process of initializing the service, the random number read from the IC card 100 is used only for generating the initial password and, after the initial one, the random number is increased by one when each password is generated at step 650. When the counter value N becomes 0, a random

number generated during the generation of the password (for example, the resultant value of the symmetrical key cipher algorithm) is set as the random number initialized value. The password is generated by increasing the random number by one at step 650. A new random number is set when the counter value N becomes 0 at step 660. After generating a password, the counter value N and the random number RN are recorded in the random number memory 122 at step 670..

(Col. 10, lines 43-61, emphasis added through underlining). Yu further states that the “one-time password is generated using the secret key (secret keys for the symmetrical key cipher algorithm), shared by the IC card 100 and the server 140, and also using a random number value.” (Col. 10, lines 1-4). Thus, according to Yu, the random number value which is reset is different from the secret key which is not reset. Therefore, Yu fails to teach, suggest, or describe “wherein the number of identifications allowed is based on a maximum number of times the secret value may be used before the secret value is changed” or “based on an outcome of the comparison, identifying a second secret value” (emphasis added through underlining) as recited in Claims 29, 36, and 42.

As a result, Applicants respectfully submit that Claims 29, 36, and 42 are patentable over Montenegro in view of Yu. The remaining claims depend from one of Claims 29, 36, and 42. Therefore, Applicants respectfully request withdrawal of the rejection of Claims 29-32, 35-39, 41-45, and 47 under 35 U.S.C. § 103(a).

Applicants believe that the present application is in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by the credit card payment instructions in EFS-Web being incorrect or absent, resulting in a rejected or incorrect credit card transaction, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely

acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date September 25, 2008

FOLEY & LARDNER LLP
Customer Number: 23524
Telephone: (608) 258-4263
Facsimile: (608) 258-4258

By _____

Callie M. Bell
Attorney for Applicant
Registration No. 54,989